CLAIMS

1. Conditional access data decryption system, this system comprising:

- a diffusion centre (10) arranged to diffuse data encrypted by at least one control word (cw),
- at least one management centre (11) arranged to diffuse personal messages (ECM, EMM) related to the management of access means to encrypted data,
- an operating device (12) intended to render usable said encrypted data, and
- a decoder (13) arranged to decrypt at least one part of the encrypted data, placed between the diffusion centre (10) and the operating device (12),

characterized in that

- the decoder (13) comprises a module (14) for the reception and decryption of encrypted data and a module (15) for the management of access rights to this data, these modules being physically different, the reception module (14) being connected to the operating device (12) and the management module (15) being arranged to communicate with the reception module,
- the management module (15) includes a security module (16) comprising a unique identification number (UA) and data allowing securing the connection between said management centre (11) and the security module (16), this security module being arranged to verify the content of the personal messages (ECM, EMM) and to allow or prevent the decryption of the control-word(s) (cw) according to the content of the personal messages,
- and in that the reception module (14) receives the encrypted data originating from the diffusion centre (10) via a first communication line, and the management module (15) receives the personal messages (ECM, EMM) through the management centre (11) via a second communication line.

2. Data decryption system according to claim 1, **characterized in that** the communication between the reception module (14) and the management module (15) is a communication by means of waves.

3. Data decryption system according to claim 1, **characterized in that** the rights management module (15) is a mobile telephone.

4. Data decryption system according to claim 3, **characterized in that** the security module (16) includes identification functions necessary for telephony and at least one storage area pertaining to a management centre (11), this area comprising the security parameters for reception of the authorization messages (EMM) of said management centre.

5. System according to claims 1 to 4, **characterized in that** the diffusion centre (10) is arranged to diffuse control messages (ECM) comprising the control-word(s) (cw), and in that the personal messages broadcasted by the management centre (11) correspond to an authorization message (EMM).

6. System according to claims 1 to 4, **characterized in that** the management centre (11) is arranged to diffuse personal messages comprising the control-word(s) (cw), the security module (16) of the management module (15) having means to determine if this message is intended for said security module and means to transmit this control word (cw) to the reception module (14).

7. System according to claim 6, **characterized in that** the reception and decryption module (14) includes a unique decryption key applied to the control word (cw), this key serving to encrypt the control-words at the management centre (11) before their transmission towards the management module (15).

8. Data decryption system according to claim 1, including at least two management centres (11), **characterized in that** the security module (16) of the managing module (15) includes security parameters for the reception of the authorization messages (EMM) originating from different management centres (11).

9. Data decryption system according to claims 1 to 8, the diffusion centre (10) being arranged to transmit descriptive information of the encrypted data, **characterized in that** this data contains indications necessary for the establishment of communication with the management centre (11) that is responsible for the authorization of this data, and is transmitted to the management module (15), the latter being arranged to establish communication with the management centre (11) in question to obtain the authorization message (EMM).

10. Data decryption system according to one of the previous claims, **characterized in that** the reception and decryption module (14) is integrated into the operating device (12).

11. Data decryption system according to claim 1, **characterized in that** the reception and decryption module (14) includes standardized communication means with the management module (15) so that a reception and decryption module (14) can interact with a plurality of management modules (15).

12. Data decryption system according to one of the previous claims, **characterized in that** the management module (15) includes means to establish a matching key with the reception module (14), this key being intended to encrypt and decrypt at least the control-word(s) (cw) transmitted to the management module (15) towards the reception module (14).